CONFERENZA NAZIONALE

SICUREZZA E LEGALITÀ

Napoli 16-18 novembre 2018

Tavolo tematico: CYBER SECURITY

(Avv. Roberto De Vita –Presidente Osservatorio Cyber Security Eurispes)

I lavori del tavolo tematico Cyber Security hanno preso l'avvio dal tema generale già rassegnato nella sinossi preparatoria dell'approfondimento, tracciata dal Presidente dell'Osservatorio Cyber Security di Eurispes, Prof. Roberto De Vita, e dall'introduzione dei lavori in occasione della sessione plenaria.

In particolare, le linee guida hanno posto centralità sulla definizione dell'ecosistema digitale come bene comune e della necessità della sua protezione collettiva e diffusa. Tale approccio ha consentito di iniziare ad affrontare le tematiche della cyber security, nelle varie declinazioni, secondo punti di vista differenti da quelli comunemente utilizzati. Il dibattito ha spaziato, infatti, dall'analisi dei fenomeni, degli scenari attuali e della realtà normativa e tecnica/tecnologica per giungere alle prospettive sul futuro: da tema apparentemente solo tecnico/tecnologico a questione centrale inerente a democrazia, economia, società e diritti fondamentali.

Tale impostazione ha trovato piena conferma di validità attraverso i contributi e confronti dei relatori presenti, i quali hanno messo in evidenza di come ci si stia adeguando molto lentamente agli innumerevoli cambiamenti del mondo digitale e come, pur a fronte dei vantaggi derivanti dall'utilizzo delle tecnologie della c.d. terza piattaforma (cloud, social media, mobility, big data&analytics) e delle tecnologie che poggiano su essa (IoT, robotica, Intelligenza Artificiale, realtà aumentata e virtuale, blockchain ovvero i c.d. "Acceleratori dell'Innovazione"), gli investimenti (economici e, soprattutto, culturali) siano ancora limitati – e, spesso, scarsamente finalizzati – e come vi siano moltissimi punti critici da risolvere in relazione ai sempre maggiori rischi conseguenti.

Dalla manipolazione del consenso e condizionamento delle scelte degli individui, al condizionamento delle democrazie e dei Paesi fino ad arrivare al rischio per le infrastrutture critiche, alla protezione dei dati e alla sicurezza dei processi di automazione dell'Operation Technology.

Il Dr. Quacivi (Sogei) ha evidenziato come la minaccia cibernetica costituisca uno dei principali rischi che le diverse organizzazioni si trovano ad affrontare, facendo specifico riferimento all'ambito della Pubblica Amministrazione e alle piccolissime, piccole e medie imprese.

Ed infatti, a fronte della tendenza delle imprese ad effettuare investimenti in termini di business, non vi è una corrispondente proiezione sulla protezione dei dati e sulla sicurezza aziendale. E se le grandi aziende si stanno dotando dei necessari sistemi di protezione, la rilevante quota delle PPMI italiane rimane isolata rispetto a questo bisogno.

Tale aspetto ha ricevuto ulteriore conferma da parte dell'Ing. Bordi (Leonardo) e del Dr. Morelli (Terna), con specifico riferimento ai rischi di vulnerabilità strutturale e, soprattutto, comportamentale, della supply chain e della filiera produttiva, evidenziando l'indispensabilità della

condivisione e del partenariato pubblico/privato e privato/privato, confermando come la protezione dei rischi debba avere un approccio integrato e sistemico.

Il dibattito, proprio in relazione a tale key issue, ha sottolineato l'indispensabilità di una condivisione e trasferimento di modelli, processi e best practices dal player pubblico e dalle industrie strategiche agli operatori più piccoli e periferici, tipicamente non dotati di risorse strutturali e specializzate per fronteggiare i rischi cibernetici.

Diversi relatori hanno anche evidenziato come solo attraverso la condivisione delle esposizioni concrete a minacce in tutto l'ecosistema digitale sia possibile realizzare un flusso informativo che alimenti in chiave di intelligence analysis la tutela del sistema Paese.

L'Ing. Bordi ha tracciato lo schema simmetrico "persone-processi-tecnologie" come linea guida fondamentale. In tal senso tutti i relatori hanno affrontato il tema della debolezza – e conseguente necessità di intervento – della e sulla consapevolizzazione (awareness) che contraddistingue l'approccio basilare di protezione; pertanto, la cyber security delle organizzazioni e delle imprese non può prescindere dalla formazione dei soggetti che interagiscono con l'ecosistema digitale, sia nei comportamenti aziendali che nei comportamenti privati (ne sono un esempio le social media policies).

Altro tema centrale introdotto dal Prof. De Vita e oggetto di approfondimento - e declinazione multidisciplinare - ha riguardato l'Intelligenza Artificiale (AI) e i sistemi avanzati ed automatizzati che sfruttano tecnologie di machine learning per l'automazione dei processi di analisi e dei processi decisionali.

Il Prof. Loia (Università di Salerno) ha in particolar modo evidenziato come le tecnologie che consentono ai computer di apprendere e adattarsi al contesto in cui operano, emulando la cognizione umana nella sua capacità di apprendere basandosi sull'esperienza piuttosto che sul ragionamento deduttivo, stanno assumendo ruolo dominante nel mondo digitale perché consentono alle macchine di elaborare in modo autonomo la costruzione di modelli complessi di interpretazione della realtà.

Il dibattito, quindi, si è incentrato sulle applicazioni concrete dell'AI e del machine learning ai settori della difesa militare, della predizione comportamentale, della business intelligence and operation, della cyber risk response, fino ad arrivare ai rischi che la sostituzione delle macchine agli uomini nel processo decisionale comporta. Rischi relativi sia alla definizione delle regole fisiche ed etiche di comportamento dell'AI, sia alla modificazione dei pesi strategici dei Paesi in ambito economico e militare, derivanti dagli investimenti massivi che alcuni Paesi hanno fatto e stanno facendo, recuperando gap tecnologici ed economici rispetto a posizioni di società avanzate, il cui stato di maturità tecnologica ed economica si accompagna già ad un avvenuto consolidamento di diritti fondamentali e di funzionamento democratico.

L'Intelligenza Artificiale è risorsa indispensabile, così come lo sono allo stato attuale gli algoritmi, per poter processare e ricavare significato da una sempre maggiore mole monstre di dati (Big Data) e per poter ridurre a tendente zero la capacità di immediatezza della risposta decisionale.

Tuttavia, come ben sottolineato dal Prof. Caligiuri (Università della Calabria) questo sta determinando – oltre ad una modificazione strutturale e definitiva degli assetti geopolitici del

Novecento – un progressivo processo di irrilevanza della partecipazione umana ai processi decisionali più complessi, tra i quali l'esercizio della democrazia, così prefigurando scenari di artificial governance delle relazioni umane e sociali.

Tale tema, apparentemente suggestivo e futuribile, è stato oggetto di lungo confronto ed ha ricevuto particolare attenzione – proprio in relazione alla manipolazione del consenso, al rischio per le democrazie e per le relazioni tra Paesi, al condizionamento per le relazioni individuali – nelle riflessioni che il Direttore della Polizia Postale e delle Comunicazioni, Dr.ssa Ciardi, ha condiviso con la tavola rotonda, anticipando un argomento di particolare rilevanza inerente l'impreparazione antropologica degli individui rispetto al passaggio dalla sovrastruttura analogica (sociale, economica politica e giuridica) a quella digitale, con conseguente esposizione al rischio strutturale della fragilità del mondo come sino ad oggi conosciuto.

Queste ultime riflessioni hanno poi guidato la parte del dibattito relativa al contributo del Prof. Simons (Istituto Studi Russi ed Euroasiatici) che ha evidenziato le differenze tra il flusso informativo, la disinformazione e i sistemi di aggregazione del consenso nel mondo fisico, analogico e in quello digitale, confermando come non sia più sostenibile la distinzione tra identità e agire digitale e identità e agire fisico.

I contributi hanno poi affrontato temi di immediato allarme sociale, legati a pedopornografia e cyber bullismo, web reputation e temi di rilevanza strategica riguardanti le sempre più macro dimensionate aggressioni ai sistemi finanziari, come sottolineato dalla Dr.ssa Ciardi. Analoga posizione è stata espressa dal Dr. Luca Danese di Eurispes in una riflessione sui sistemi bancari, il quale ha rilevato come, a fronte di minacce crescenti, la risposta in termini di definizioni e regole sia ancora di là da venire.

Nell'affrontare poi le nuove emergenze relative al cyber money laundering, alle nuove forme di sfruttamento delle piattaforme di comunicazione da parte dei cyber terroristi (fenomeno non legato solo a propaganda, reclutamento e finanziamento ma come proiezione di offesa a strutture critiche e strategiche), il Prof. De Vita ha riportato gli approfondimenti dell'Avv. Guerrisi e dell'Avv. Laudisa del gruppo di ricerca dell'osservatorio Cyber Security di Eurispes, i quali hanno infatti descritto, nel paper offerto come contributo specialistico alla tavola rotonda, oltre ai temi già in precedenza tracciati, lo stato attuale degli sforzi (in termini di regole) che contesti sovranazionali, quali l'Unione Europea, ed internazionali hanno fatto negli ultimi anni, nonché gli investimenti nello sviluppo del partenariato nel law enforcement pubblico e privato. Per poi proseguire sui protocolli di intesa proiettati dall'Unione Europea nel 2018 per il contrasto alle fake informations, agli algoritmi manipolatori non trasparenti e ai sistemi automatizzati di amplificazione della visibilità politica attraverso piattaforme social, in vista delle prossime elezioni europee del 2019.

Di particolare interesse, per la rilevanza del contributo tecnico, sul tema da ultimo affrontato, la relazione del cyber warfare specialist Francesco Zorzi, il quale ha descritto in chiave accessibile i meccanismi di funzionamento degli algoritmi, dei sistemi decisionali e di predizione e profilazione, portando esempi concreti: dal riferimento alle piattaforme di comunicazione più diffuse e ai sistemi distribuiti di acquisizione di dati, alle modalità attraverso cui l'ingegneria sociale (integrata alle metodiche di attacco organizzato) consente, dalla periferia al centro, di portare attacchi alle infrastrutture critiche protette strategicamente, confermando quindi come la protezione non possa essere oggetto di delega tecnica ma debba avere nella consapevolizzazione del rischio comportamentale lo strumento di principale difesa.